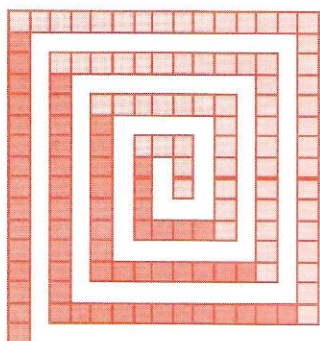




Number Theory

Bookmark 1 Foundations

Section 1 gives a very brief introduction to the whole course and, in particular, illustrates the sort of problem that will be encountered as the course progresses.

Section 2 introduces various families of numbers which will appear in the course, including the triangular numbers and the squares. It goes on to explore some relationships between these families of numbers.

Objectives

- to be able to generate sequences of numbers arising from geometrical patterns;
- to be able to write down the general term of a sequence of numbers given the pattern generating the sequence;
- to be able to use the formulae for sums of arithmetic series in summing given series.

Section 3 introduces Mathematical Induction. This powerful method of proof will be used many times in the course and it is important that you come to terms with it at this stage. The section includes some theory, and justification of the soundness of induction, but you should regard induction primarily as a technique to be mastered and hence your effort should be directed at understanding the examples of its use and practising induction proofs yourself.

Objectives

- to be familiar with the standard set notations used in this course;
- to understand the Principle of Mathematical Induction, and be able to use it in proving propositions of a variety of kinds with the common feature that they assert the truth of some result for all integers greater than some given value;
- to understand the Second Principle of Mathematical Induction and recognize situations in which proof by induction is more amenable to the use of the Second Principle.

Section 4 establishes key divisibility properties of integers and develops properties involving the important notion of the greatest common divisor (gcd) of two integers. There are many relatively straightforward results in this section but these will be used time and time again. Therefore you should not rush the section and be prepared to refer back to it frequently, until using the properties becomes almost second nature to you.

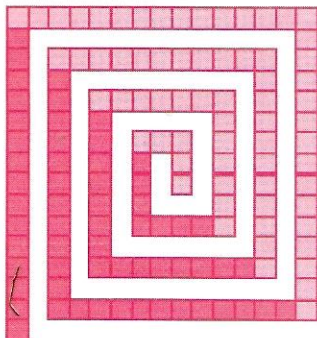
Objectives

- to be familiar with the Division Algorithm and be able to determine the unique remainders on dividing by some positive integer n ;
- to be familiar with, and be able to use, the divisibility properties of integers as given in Theorems 4.2, 4.6 and 4.7;
- to understand what is meant by the greatest common divisor of two integers and appreciate and be able to use the various properties involving $\gcd(a, b)$;
- to understand what is meant by two integers being relatively prime;
- to understand what is meant by the least common multiple (lcm) of two integers.

Section 5 should prove to be a relatively light section. The Euclidean Algorithm is introduced as a way of determining the gcd of two integers and, looked at in a different way, as a means of solving linear Diophantine equations.

Objectives

- to be able to use the Euclidean Algorithm to determine the greatest common divisor of two given integers;
- to recognize when a linear Diophantine equation has solutions, and when it does not;
- to be able to find particular and general solutions of given linear Diophantine equations through the application of the Euclidean Algorithm.



Number Theory

Bookmark 2 Prime Numbers

Section 1 introduces prime numbers and is concerned with the basic properties of primes. The results of Theorems 1.1, 1.2 and 1.3 and its Corollary, probably seem obvious facts, but they will be used continually throughout the remainder of the course and so you must, at this stage, appreciate them fully and practise using them in the problems provided. The Fundamental Theorem of Arithmetic, which spells out the unique way of breaking any positive integer down into primes, is also something you may well have taken for granted previously. But it is an important theoretical result which will be appealed to time and time again.

Objectives

- to appreciate the notion of a prime number and be able to use the divisibility properties, presented in the theorems of the section, in a variety of situations;
- to appreciate that any integer greater than 1 can be broken down into prime power divisors in a unique way, and be able to produce this prime decomposition for a given integer;
- to understand the proof of the Fundamental Theorem of Arithmetic.

Section 2 is a relatively short section concerned with the set of divisors of an integer whose prime decomposition is given. The section hinges on one result, Theorem 2.1, which shows how to list all divisors of the given integer. As an offshoot we know exactly how many divisors an integer has, and this is captured in Theorem 2.2, where it is expressed in terms of the τ function (which we pursue further in *Unit 5*).

Objectives

- to be able to list all divisors of an integer from its prime decomposition;
- to be able to write down the $\gcd(m, n)$ and the $\text{lcm}(m, n)$ when the prime decompositions of m and n are given;
- to appreciate the formula for the τ function and be able to use it to determine integers with a given number of divisors.

Section 3 is concerned with occurrences of prime numbers in the sequence of positive integers, beginning with Euclid's classical proof that there are infinitely many primes. The section then turns to the question of primes in an arithmetic progression, building up to Dirichlet's Theorem which is the ultimate result in this area. In this course we only prove special cases of this theorem, including Theorem 3.3 and Problem 3.3. Other particular cases will be proved later, using variations on the arguments introduced here. The section concludes by looking at

some instances of primes generated by functions. Theorem 3.5 is included for completeness, but its proof, which requires techniques from Calculus, may be treated as optional reading.

Objectives

- to be able to reproduce Euclid’s proof of the infinitude of primes;
- to be familiar with the result of Dirichlet’s Theorem;
- to be able to prove that there are infinitely many primes in certain arithmetic progressions.

Section 4 is a short section discussing some famous problems, both solved and unsolved, involving primes. You should be able to work through this section reasonably quickly as the section is included primarily for interest with no substantial technical work to be digested.

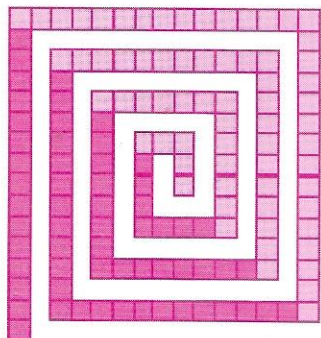
Objectives

- to be able to prove that, in the set of integers, there are unlimited sequences of composite numbers;
- to understand the notions of twin prime, prime triple and prime quartet;
- to appreciate the results of Goldbach’s Conjecture and the Prime Number Theorem.

Section 5 comprises a brief introduction to Fibonacci numbers and their properties. (There are many further properties of interest which we shall not encounter in this course.) Attention here is on the divisibility properties of Fibonacci numbers and, to maintain the connection with primes, an investigation of where primes crop up amongst the Fibonacci numbers. The notion of a remainder sequence illustrates the concept of congruence which is the theme of the next unit.

Objectives

- to be able to determine which Fibonacci numbers are multiples of any given positive integer, through investigation of the remainder sequence;
- to be familiar with the basic properties of Fibonacci numbers and be able to use these properties to establish other given identities involving Fibonacci numbers.



Number Theory

Bookmark 3 Congruence

Section 1 introduces the topic of congruence. You should find that the material in this section is straightforward. However, the properties of congruence (as listed in this section's theorems), and the uses to which they are going to be put throughout the remainder of the course, make this section very important. Do not rush it, and do try all the problems as practice in using congruence ideas will be essential.

Objectives

- to understand the notion of congruence and be able to compute values in the arithmetic modulo n using the properties of Theorem 1.1;
- to understand what is meant by a complete set of residues, the set of least positive residues and the set of least absolute residues, and appreciate the role played by a complete set of residues in problems in arithmetic modulo n ;
- to understand the results of Theorems 1.3, 1.4 and 1.5 and appreciate how to use them in congruence problems.

Section 2 is a short section with the goal of using congruence ideas to explain how, and why, various divisibility tests work.

Objectives

- to be able to use divisibility tests, in particular those for divisibility by 9 and 11, and explain why they work.

Section 3 turns to the subject of linear congruences. As the course progresses we shall witness numerous problems, from diverse areas of number theory, which can be attacked by congruence methods, and solving linear congruences is something which will crop up frequently. Although this section contains some essential theory concerning the solutions of linear congruences, it is really about techniques for solving them and your main effort should be directed towards practising these through the problems provided.

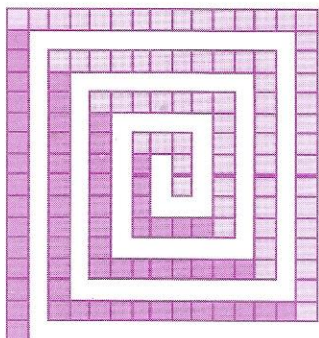
Objectives

- to appreciate what is meant by distinct solutions of a linear congruence;
- to recognize how many solutions a linear congruence has and, in particular, be aware when a linear congruence has no solutions;
- to be able to apply the suggested strategy to solve any given linear congruence (for reasonably sized coefficients and modulus).

Section 4 takes linear congruences one step further and investigates a range of problems each of which can be modelled as a system of simultaneous linear congruences. Attempting to solve such a system leads us to one of the classical theorems of number theory, the so-called Chinese Remainder Theorem. The given proof of this theorem actually constructs a solution of the system in question, but it is a cumbersome construction and the section goes on to suggest an alternative, simpler way of finding solutions. The section ends by giving a necessary and sufficient condition for such a system of congruences to have a simultaneous solution.

Objectives

- to appreciate the Chinese Remainder Theorem, and be able to use the construction given in its proof to solve systems of simultaneous linear congruences in which the moduli are relatively prime in pairs;
- to be able to use the alternative method to that above, as illustrated in Example 4.3 and Problem 4.2, to solve systems of simultaneous linear congruences;
- to be aware of the conditions under which a system of simultaneous linear congruences will have a solution when the moduli are not relatively prime in pairs, and to be able to find the solution in such circumstances.



Number Theory

Bookmark 4 Fermat's and Wilson's Theorems

Section 1 introduces one of the most important theorems in number theory: Fermat's Little Theorem (FLT). This theorem, its proof, and the applications given here should prove to be uncomplicated reading, but FLT is going to be used so frequently in what follows that this section should not be rushed. The final subsection turns to the converse of FLT, which is seen to be false, although numbers which provide a counter-example are not easy to find.

Objectives

- to appreciate and be able to prove Fermat's Little Theorem;
- to be able to use FLT in a variety of situations, in particular, to be able to determine the remainder when any power of any number is divided by a (none-too-large) prime;
- to understand the converse statement of FLT and be able to explain why it is false.

Section 2 is concerned with the decimal expansions of fractions. Its main purpose is to illustrate the use of FLT in explaining phenomena which may well be known to you, namely why the decimals of some fractions terminate while others have cycles of digits which repeat indefinitely. There is a good deal of technical information presented in the section, and a number of areas are left incomplete. However this section can be worked through quickly, the only important concept for future work being that of 'order of an element'.

Objectives

- to be able to calculate the decimal of any given fraction;
- to appreciate which fractions have terminating decimals;
- to understand the notion of, and be able to calculate, the order of an element modulo a prime;
- to be able to explain why the cycle length in the decimal of proper fraction $\frac{r}{p}$ is equal to the order of 10 modulo the prime p .

Section 3 is a short section presenting a second classical result, Wilson's Theorem, which shares with FLT the fact that both are concerned with reducing the values of large numbers modulo a prime. However the use of Wilson's Theorem in computations is very limited and it will be seen here, and subsequently, that it tends to be mainly a result with theoretical applications. Unlike the situation with FLT, the converse of Wilson's Theorem is seen to be true.

Objectives

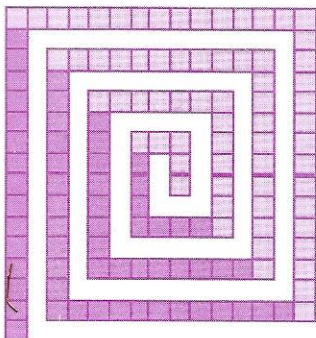
- to understand and be able to prove Wilson’s Theorem;
- to appreciate that the converse of Wilson’s Theorem is true, and be able to prove it.

Section 4 returns to the theme of polynomial congruences, touched on briefly in the previous unit. The question which dominates our attention concerns how many solutions a polynomial congruence with prime modulus can have, and our goal is a theorem of Lagrange which says that the number of solutions cannot exceed the degree of the congruence. The section looks at some methods of solving polynomial congruences with either prime or composite modulus. In doing so it gives some of the flavour of techniques available, but stops some way short of a systematic treatment of what is a vast area of investigation.

Objectives

- to be able to solve polynomial congruences of small degree and modulus by trial and error methods;
- to appreciate the result of Lagrange’s Theorem;
- to be aware that, for a polynomial congruence with prime modulus, each solution corresponds to a linear factor of the polynomial modulo p and, for congruences of small degree and modulus, be able to factorize the polynomial modulo p ;
- to be able to solve a polynomial congruence of small degree and composite modulus n by first solving the congruence modulo each of the prime divisors of n .

Section 5 rounds off the unit by showing how each of FLT and Wilson’s Theorems can be demonstrated by appropriate counting in a couple of well-known combinatorial problems. There is no new material in this section other than the examples themselves.



Number Theory

Bookmark 5 Multiplicative Functions

Section 1 introduces multiplicative functions, which we shall discover are very useful functions in number theory. The section concentrates on two examples of multiplicative functions: the τ function which counts the number of positive divisors of an integer and, allied to it, the σ function which adds up those positive divisors. The multiplicative property leads to a fairly simple formula which gives the value $\sigma(n)$ from the prime decomposition of n .

Objectives

- to understand what a multiplicative function is and to be able to use the multiplicative property to determine values of a given multiplicative function;
- to appreciate why the τ function and the σ function are multiplicative;
- to be able to derive the prime decomposition formula for σ from the multiplicative property;
- to be able to use the prime decomposition formulae to determine values of $\tau(n)$ and $\sigma(n)$.

Section 2 is concerned with perfect numbers. The search for perfect numbers has an interesting history, which we have attempted to highlight in this section. Pursuit of perfect numbers leads us to a discussion of the Mersenne primes and then to Fermat numbers. Although there is a good deal of technical information presented here, after the first subsection there is little that needs to be mastered and so you should be able to work through this section reasonably quickly.

Objectives

- to understand what is meant by perfect numbers and be able to give some examples;
- to be able to deduce the classification of even perfect numbers;
- to appreciate Mersenne primes and their connection with perfect numbers and be aware of some tests for the primality of Mersenne numbers;
- to appreciate Fermat numbers and the difficulties encountered in testing their primality.

Section 3 introduces another multiplicative function, Euler's ϕ -function, and goes on to present Euler's Theorem, which generalizes FLT to cater for the case of composite modulus. The rest of the section is devoted to a variety of applications of Euler's Theorem, in particular, using the notion of the order of an integer (which is also generalized to have meaning when the modulus is composite). Repunits are introduced as an interesting example to illustrate an application of Euler's Theorem.

Section 3 is the most important section of the unit and should not be rushed.

Objectives

- to understand what is meant by a reduced set of residues and be able to write down such a set for any given modulus;
- to appreciate Euler's ϕ -function and be able to compute $\phi(n)$ for small positive integers n ;
- to understand, be able to prove and use Euler's Theorem;
- to understand what is meant by the order of an integer modulo some positive integer and be able to determine the order of an integer to any given (not too large) modulus.

Section 4 is mainly concerned with two results. First a proof is given of the fact that Euler's ϕ -function is multiplicative. The underlying idea behind this proof is straightforward but the details are a little cumbersome. You should work through the proof once but you will not be expected to reproduce it. With the multiplicative property of ϕ available, the second result uses it to obtain a formula for $\phi(n)$ from the prime decomposition of n .

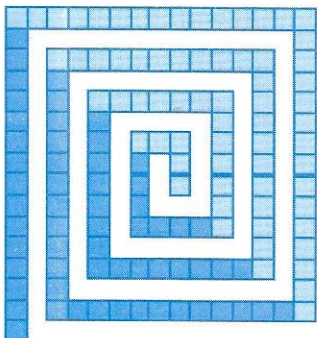
Objectives

- to be aware that Euler's ϕ -function is multiplicative;
- to be able to derive a formula for $\phi(n)$ in terms of the prime decomposition of n , from the multiplicative property;
- to be able to use the formula to determine values of $\phi(n)$;
- to be able to use the multiplicativity of ϕ and the formula for $\phi(n)$ in a variety of situations.

Section 5 pursues the theme of the order of an integer in arithmetic modulo n , focussing on the concept of a primitive root, that is, an integer which has the maximal possible order given by Euler's Theorem. The final subsection answers the question of which moduli admit primitive roots, a result which is of great importance in the study of finite fields. Here however, the subsection is included for completeness and may be regarded as optional reading.

Objectives

- to understand the notion of a primitive root and decide whether or not a given integer is a primitive root of n ;
- given a primitive root of n , to be able to determine the order of each integer modulo n and, in particular, be able to find all primitive roots of n ;
- to be aware of precisely which moduli n admit primitive roots.



Number Theory

Bookmark 6 Quadratic Reciprocity

Section 1 broaches the question of whether or not a quadratic congruence with prime modulus p has solutions. This leads us to investigate which numbers in the set of non-zero least positive residues modulo p are 'squares'. The main result of the section, Euler's Criterion, provides one way of solving this particular problem. We shall see many applications of Euler's Criterion here and in the coming sections.

Objectives

- to understand the terms quadratic residue, quadratic non-residue and quadratic character;
- to be able to solve quadratic congruences in which the prime modulus is reasonably small;
- to be able to determine all the quadratic residues of a given (not too large) prime;
- to understand and be able to prove Euler's Criterion;
- to be able to determine all the quadratic residues of a given prime from a known primitive root.

Section 2 introduces important new terminology: the Legendre symbol (a/p) . Theorem 2.1 expresses results discovered in Section 1 in terms of the Legendre symbol. The remainder of the section is devoted to using the five properties of Theorem 2.1 in the investigation of quadratic congruences. This is a short, but important section.

Objectives

- to understand and be able to use the Legendre symbol;
- to be fully aware of the five properties of Theorem 2.1 and be able to use them in the evaluation of Legendre symbols and related problems.

Section 3 is concerned with Gauss' Lemma, a result which will be seen to be useful in its own right as well as being a key stage along the way to proving the Law of Quadratic Reciprocity. The underlying idea behind our proof of Gauss' Lemma is interesting, and not very complicated, and so one of your objectives for the unit will be to be able to reproduce this proof. Amongst numerous applications of Gauss' Lemma, we shall establish several more special cases of Dirichlet's Theorem which we first met in *Unit 2*.

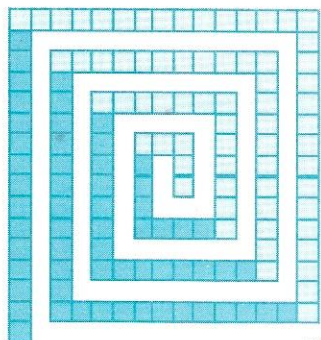
Objectives

- to understand and be able to prove Gauss' Lemma;
- to be able to use Gauss' Lemma to calculate Legendre symbols involving a reasonably small prime modulus;
- to appreciate why any Legendre symbol can be calculated once the values of $(-1/p)$, $(2/p)$ and (q/p) can be determined for any odd primes p and q ;
- to be able to write down the values of $(-1/p)$ and $(2/p)$ for any given odd prime p ;
- to be able to prove some special cases of Dirichlet's Theorem;

Section 4 turns to the big result of the unit, the Law of Quadratic Reciprocity, which will enable you to evaluate any Legendre symbol (a/p) . It is followed by a number of simple applications. You will not be asked to reproduce the proof of the Law of Quadratic Reciprocity, and so your efforts should be directed towards understanding the result, and knowing how to use it. Nevertheless, the result is of such fundamental, and historic, importance that we recommend that you work through the given proof once. The Jacobi symbol is mentioned for completeness but it is non-examinable.

Objectives

- to understand the Law of Quadratic Reciprocity;
- to be able to calculate any Legendre symbol (a/p) no matter how large the number a and the prime p ;
- to be able to decide whether or not any given quadratic congruence is solvable.



Number Theory

Bookmark 7 Continued Fractions

If you have not met continued fractions before you should find this unit intriguing. Although there is a fair amount of theory involved, it is more important that you should appreciate the ideas involved and the results of the theorems, and that you become proficient with the processes through tackling as many of the problems and exercises as you have time for. It is a relatively straight forward unit which should not pose you any great problems.

The Introduction gives examples of finite and infinite continued fractions in the context of the golden ratio.

Section 1 studies finite continued fractions. Although our main interest will ultimately be with infinite continued fractions, all the spadework for the unit is done in this section for, as we shall see, most of the properties discovered for finite continued fractions generalize in a natural way to the infinite case. Do not rush this section because, if you understand the properties and master the techniques taught here, you will find the rest of unit so much more straightforward.

Objectives

- to be able to determine the simple finite continued fraction of any given rational number;
- to be able to write down the sequence of convergents of a given simple finite continued fraction, finishing with the value of the fraction itself;
- to be familiar with, and be able to make use of, the various properties of the convergents of a simple finite continued fraction as listed in Theorems 1.3 and 1.4;
- to solve a given linear Diophantine equation through the use of continued fractions.

Section 2 turns to infinite continued fractions. Such entities cannot be evaluated by the normal rules of arithmetic because infinite processes are involved. This section defines what is meant by the value of an infinite continued fraction and goes on to show that every continued fraction does have a value. The rest of the section is devoted to examples of such evaluations for the case of periodic continued fractions. (Certain properties of limits, such as would be encountered in any first course in Mathematical Analysis, have to be assumed. If you are not familiar with these notions then you will have to accept some of the justifications given. This will not affect your ability to evaluate continued fractions, which is our prime concern.)

Objectives

- to understand what is meant by the value of an infinite continued fraction;
- to be able to write down an integral quadratic equation which is satisfied by a given purely periodic continued fraction, and hence to determine its value;
- to be able to evaluate any periodic continued fraction.

Section 3 establishes a one-one correspondence between irrational numbers and simple infinite continued fractions: every irrational number has such a continued fraction and conversely the value of every such continued fraction is irrational. But, this theory aside, your efforts in this section should be directed towards the practicality of finding the continued fraction of a given irrational number. The Continued Fraction Algorithm provides a means of doing this and there are plenty of examples, problems and exercises to give you practice in its use.

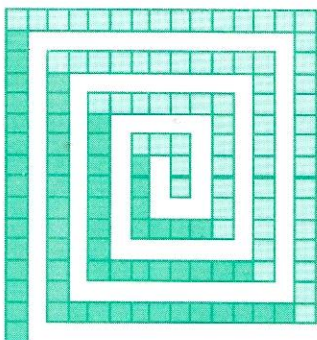
Objectives

- to understand, and be able to use, the Continued Fraction Algorithm;
- to determine some of the leading partial quotients in the continued fraction of any given number, and hence some of its leading convergents;
- to be able to determine the (whole) continued fraction of certain irrational numbers, including $\sqrt{n}$, for any non-square positive integer n .

Section 4 investigates the role played by continued fractions in finding rational approximations to real numbers. It transpires that the convergents in the continued fraction of a number are the ‘best possible’ approximations in a sense clarified in the section. The corollary to Theorem 4.1, which gives bounds to the accuracy of using convergents as an approximation to a number, is the crucial result of this section; you should appreciate it and become comfortable using it. The section ends by demonstrating how to obtain ‘best’ rational approximations to irrationals, including π , and how to recognize that a given approximation is the best possible for a given limit on the size of the denominator. The proofs in this section are technically rather tricky, so we shall not expect you to be able to reproduce them.

Objectives

- to be aware of the sense in which the convergents of a number are its best rational approximations;
- to be able to estimate the accuracy of a convergent, determining both an upper and a lower bound on its error;
- to be able to use Theorem 4.3 to recognize when a rational approximation to a number is a convergent;
- to be able to determine a rational approximation to a given number to within a given accuracy.



Number Theory

Bookmark 8 Diophantine Equations

This final unit of the course introduces the study of Diophantine equations which is a vast branch of number theory generating considerable activity. We are concerned with finding positive integer solutions of algebraic equations, and we shall quickly discover that even a relatively simple equation can be extremely difficult to resolve: that is, to find some, or all of its solutions or, alternatively, to prove that it cannot have any solutions. In this unit we shall concentrate on four famous equations and related problems.

Section 1 looks at Pell's equation, $x^2 - ny^2 = 1$. We shall learn how to solve this equation using the convergents of the continued fraction of $\sqrt{n}$, by taking advantage of some of the results from the previous unit. In places the proofs in this section do get quite technical. You will not be asked to reproduce any of the heavy proofs, so you are at liberty to cut some corners here. Your prime objective is to be able to solve any given example of Pell's equation.

Objectives

- to recognize which convergents in the continued fraction of $\sqrt{n}$ lead to solutions of $x^2 - ny^2 = 1$, and be able to determine some of these solutions;
- to recognize when $x^2 - ny^2 = -1$ has solutions and to be able to find solutions when they exist;
- to be able to find further solutions, when given the fundamental solution of $x^2 - ny^2 = 1$, by using the result of Theorem 1.3;
- to be able to use Theorem 1.4 to find solutions to each of the equations $x^2 - ny^2 = -1$ and $x^2 - ny^2 = 1$ when the cycle of $\sqrt{n}$ has odd length.

Section 2 gives a complete solution of the Pythagorean equation, $x^2 + y^2 = z^2$, and looks at a number of related problems concerning various combinations of numbers which can arise in solutions. Theorem 2.1 is the key result of the section. You should understand it, and how to use it, for it will be needed again in later sections.

Objectives

- to understand Theorem 2.1 and be able to use it to find primitive solutions of the Pythagorean equation;
- to appreciate how to find all solutions of the Pythagorean equation from the primitive ones.

Section 3 turns to what is certainly one of the most famous results in the whole of mathematics. Fermat's Last Theorem states that the Diophantine equation $x^n + y^n = z^n$ has no positive solutions for $n > 2$. The section looks at some special cases of this result and, to assist in proving that certain equations have no solutions, introduces a new method of proof called Fermat's method of infinite descent. In addition to appreciating the main results of the section, one important objective is to understand this method of infinite descent. Some of the proofs in the section are once again quite lengthy and there is no need for you to master them. However you should read the proofs with the minimum aim of appreciating how the method of infinite descent is used.

Objectives

- to understand the method of infinite descent and be able to use it in certain settings to prove that a given Diophantine equation has no solutions;
- to be familiar with Fermat's Last Theorem and to appreciate why its proof reduces to the cases $n = 4$ and $n = p$ (an odd prime);
- to be able to sketch a proof that $x^4 + y^4 = z^4$ has no positive solution.

Section 4 looks at the problem of representing integers as a sum of first two, then three, and finally four squares. The two squares problem is solved completely, by establishing for which integers n the equation $x^2 + y^2 = n$ has solutions. Our proof again involves the method of infinite descent. It is not difficult to classify those integers which can be expressed as a sum of three squares, though we present only part of the proof here. The final result along this strand is that every positive integer can be written as a sum of four squares, but the proof of this classical result is beyond the scope of the course.

Objectives

- to be aware of which integers can be written as a sum of two squares and, for any such integer, to be able to find one or more such representations;
- to be able to show which primes can be written as a sum of two squares in a unique way;
- to be aware of which integers can be written as a sum of three squares and be able to prove why no other integer can be so expressed;
- to be aware that all positive integers are representable as a sum of four squares.